

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2004 年 7 月 1 日 (01.07.2004)

PCT

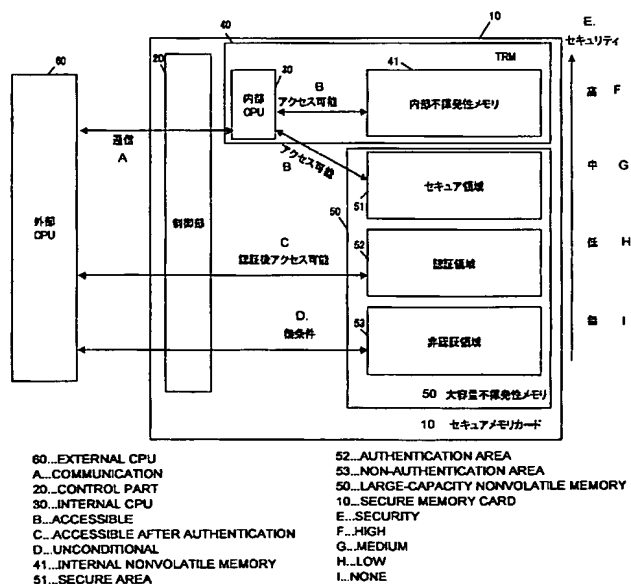
(10) 国際公開番号
WO 2004/055680 A1

- (51) 国際特許分類: G06F 12/14, G06K 19/073 (72) 発明者; および
(21) 国際出願番号: PCT/JP2003/016000 (75) 発明者/出願人 (米国についてののみ): 高木 佳彦
(22) 国際出願日: 2003 年 12 月 12 日 (12.12.2003) (TAKAGI, Yoshihiko) [JP/JP]; 〒144-0046 東京都 大田
(25) 国際出願の言語: 日本語 区 東六郷 2-2 0-5-5 0 6 Tokyo (JP). 中西 良明
(26) 国際公開の言語: 日本語 (NAKANISHI, Yoshiaki) [JP/JP]; 〒166-0014 東京都 杉
(30) 優先権データ: 2002 年 12 月 16 日 (16.12.2002) JP 並区 松ノ木 2-4-1 0-3 0 5 Tokyo (JP). 佐々木
特願 2002-363597 理 (SASAKI, Osamu) [JP/JP]; 〒144-0046 東京都 大田
(71) 出願人 (米国を除く全ての指定国について): 松下電 区 東六郷 2-2 0-5-6 2 0 Tokyo (JP). 菊地 隆文
器産業株式会社 (MATSUSHITA ELECTRIC INDUS- (KIKUCHI, Takafumi) [JP/JP]; 〒144-0046 東京都 大
TRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市 田区 東六郷 2-2 0-5-7 1 8 Tokyo (JP).
大字門真 1 0 0 6 番地 Osaka (JP). (74) 代理人: 小栗 昌平, 外 (OGURI, Shohei et al.); 〒107-
6013 東京都 港区 赤坂一丁目 1 2 番 3 2 号 アーク森
ビル 1 3 階 栄光特許事務所 Tokyo (JP).
(81) 指定国 (国内): CN, KR, US.

[続葉有]

(54) Title: MEMORY DEVICE AND ELECTRONIC DEVICE USING THE SAME

(54) 発明の名称: メモリデバイスとそれを使用する電子機器



(57) Abstract: A memory card having a large storage capacity and a memory area that has an equivalent level of security to IC cards. A semiconductor memory card (10) attachable to and removable from an electronic device has a non-tamper-resistant first memory (50) comprising ordinary areas (52,53) that are accessible from the electronic device and a secure area (51) that is not directly accessible from the electronic device, and also has a tamper-resistant second memory (41) that is not directly accessible from the electronic device. The semiconductor memory card (10) is so configured that the secure area (51) of the first memory (50) can be accessed only via a secure control part (30) that manages the access to the second memory (41). The secure area (51) cannot be directly accessed from any external device and hence exhibits a higher security level than an authentication area (52). Moreover, since the secure area (51) is provided in the non-tamper-resistant memory (50), it can have a large storage capacity.

[続葉有]



(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

— 国際調査報告書

(57) 要約: 本発明は、記憶容量が大きく、且つ、ICカードと同等のセキュリティレベルを有するメモリ領域を備えたメモリカードを提供することを目的とする。電子機器に着脱可能な半導体メモリカード10に、電子機器からアクセスすることが可能な通常領域52,53と、電子機器から直接アクセスすることができないセキュア領域51とを有する非耐タンパー性の第1のメモリ50と、電子機器から直接アクセスすることができない耐タンパー性の第2のメモリ41とを設け、第1のメモリ50のセキュア領域51へのアクセスが、第2のメモリ41へのアクセスを管理するセキュア制御部30を介してのみ可能であるように構成している。このセキュア領域51は、外部機器が直接アクセスできないため、認証領域52よりもセキュリティレベルが高い。また、このセキュア領域51は、非耐タンパー性のメモリ50に設けられるため、記憶容量を大きく取ることができる。

明細書

メモリデバイスとそれを使用する電子機器

5 <技術分野>

本発明は、半導体メモリカードなどのメモリデバイスと、このメモリデバイスへのデータの書き込み／読み出しを行う電子機器に関し、特に、セキュリティレベルが高く、大きい記憶容量を持つ記憶媒体の実現を図るものである。

10 <背景技術>

不揮発性の半導体メモリを記憶媒体として具備する半導体メモリカード（以下、「メモリカード」と言う）は、DVDなどのディスク状記憶媒体に比べて、記憶容量は小さいが、大きな機構部を必要とせず、小型で取り扱いが容易で、耐震性にも優れているため、携帯用に好適な記憶媒体として、最近、その利用範囲が拡大している。

メモリカードには、CPU（マイコン）を内蔵したものとCPUを内蔵しないものがある。CPUを内蔵したメモリカードにおけるCPUの働きは、外部機器から要求される、不揮発性メモリの読み出し・書き込み処理である。

また、メモリカードの不揮発性メモリにセキュア領域を設けて、セキュリティレベルを高める工夫も行われている。下記特許文献1には、不揮発性メモリ内に、認証に成功した外部機器のみがアクセスできる認証領域と、外部機器のいずれもがアクセスできる非認証領域とを設けたメモリカードが記載されている。このメモリカードを用いて、暗号化した音楽コンテンツを非認証領域に格納し、それを復号する復号鍵を認証領域に格納することにより、コンテンツの著作権を守ることが可能になる。

このようなメモリカードにおけるCPUの働きは、読み出し・書き込み処理に加えて、外部機器による認証領域へのアクセスを許可するための外部機器の認証処理がある。

いずれにしろ、メモリカードにおけるCPUの働きは、メモリの読み書き及びそれに付随したものに限定され、メモリに記録されたデータの制御は外部機器によって行われる。

- 5 一方、同様にCPUを内蔵するICカードは、耐タンパー性のモジュール内にCPUとともにメモリ領域を有している。耐タンパーゆえ、外部機器は、このメモリ領域に直接アクセスすることができない。そのため、ICカードは、複製や偽造に対して高い守秘性があり、高いセキュリティレベルが要求されるデジタルキャッシュのサービス等で利用されている。

- 10 ICカードにおけるCPUの働きは、メモリの読み出し・書き込みのみならず、外部から入力されたデータの暗号化、署名生成、署名検証、入力された暗証番号照合など、多岐に渡る。また、ICカードのメモリに記録されたデータの制御はICカード内部CPUによって行われる。

このように、ICカードのCPUは、従来のメモリカードに内蔵されるCPUに比べて、多機能かつ高セキュリティである。

15

〔特許文献1〕

特開2001-14441号公報

- 20 しかし、ICカードは、蓄積できる情報容量が限られており、デジタルキャッシュのサービスの多様化と共に、蓄積容量の拡大がサービス業者等から求められている。例えば、デジタルキャッシュの2重引き落とし等のトラブルを回避する目的で、電子レシートや取引ログを記録するサービスを実施しようとする、累積する電子レシート等を蓄積するために、従来のICカードの容量に比べて、大きな情報容量の確保が必要になる。

- 25 一方、前記特許文献1に記載されているメモリカードは、認証領域が可変に設定できるため、ある程度大きな情報容量を持たせることが可能である。しかし、この認証領域は、外部機器が直接制御可能な領域であるため、ICカードに比べてセキュリティレベルは低い。

<発明の開示>

本発明は、こうした従来の問題点を解決するものであり、記憶容量が大きく、
且つ、ＩＣカードと同等のセキュリティレベルを有するメモリ領域を備えたメモ
リデバイスを提供し、また、そのメモリデバイスを使用する電子機器を提供する
5 ことを目的としている。

そこで、本発明では、電子機器に固定的にまたは着脱可能に接続されるメモリ
デバイスに、電子機器からアクセスすることが可能な通常領域と、電子機器から
直接アクセスすることができないセキュア領域とを有する非耐タンパー性の第１
のメモリと、電子機器から直接アクセスすることができない耐タンパー性の第２
10 のメモリとを設け、第１のメモリのセキュア領域へのアクセスが、第２のメモリ
へのアクセスを管理するセキュア制御部を介してのみ可能であるように構成して
いる。

このセキュア領域は、外部機器が直接アクセスできないため、従来の認証領域
よりもセキュリティレベルが高い。また、このセキュア領域は、非耐タンパー性
15 のメモリに設けているため、低コストで大きい記憶容量を取ることができる。

また、本発明では、メモリ領域として第１領域、第２領域及び第３領域を有す
るメモリデバイスに対してアクセスを行う電子機器が、メモリデバイスへのアク
セス要求を受けたときに、メモリデバイスの非耐タンパー性のメモリ領域である
第１領域には、メモリデバイスへのアクセスを制御するメモリデバイスの全体制
20 御部を介してアクセスを行い、第１領域以外の非耐タンパー性のメモリ領域であ
る第２領域には、全体制御部と、第２領域及び第３領域へのアクセスを制御する
メモリデバイスのセキュア制御部とを介して、セキュア制御部との認証を経た後、
アクセスを行い、また、メモリデバイスの耐タンパー性のメモリ領域である第３
領域には、全体制御部及びセキュア制御部を介して、セキュア制御部との認証を
25 経た後、アクセスを行うように構成している。

この電子機器は、この半導体メモリカード等のメモリデバイスを活用して、多
様なサービスの実現を図ることができる。

<図面の簡単な説明>

図 1 は、本発明の実施形態におけるセキュアメモリカードの概念図；

図 2 は、本発明の実施形態におけるセキュアメモリカードの構成を示すブロック図；

5 図 3 は、本発明の実施形態におけるセキュアメモリカードを使用するシステムの概念図；

図 4 は、本発明の実施形態における R/W 装置の構成を示すブロック図；

図 5 は、本発明の実施形態におけるセキュアメモリカードの書き込み手順を示すシーケンス；

10 図 6 は、本発明の実施形態におけるセキュアメモリカードの書き込み手順の続きを示すシーケンス；

図 7 は、本発明の実施形態におけるセキュアメモリカードの他の書き込み手順を示すシーケンス；

図 8 は、本発明の実施形態におけるセキュアメモリカードの大容量不揮発性メモリの構造を示す図；

15 図 9 は、本発明の実施形態における論理—物理アドレス変換テーブルを示す図；

図 10 は、本発明の実施形態における論理—物理アドレス変換テーブルの他の例を示す図；

20 図 11 は、本発明の実施形態におけるセキュアメモリカードの大容量不揮発性メモリの異なる構造を示す図；

図 12 は、本発明の実施形態における論理—物理アドレス変換テーブルの異なる例を示す図である。

尚、図中の参照番号は、10—セキュアメモリカード；11—IC部；12—I/F部；13—ICコマンド処理部；14—ファイル管理部；15—I
25 C認証部；16—メモリ管理部；17—暗復号回路；18—内部不揮発性メモリ I/F部；20—制御部；21—データ I/F部；22—コマンド I/F部；23—制御認証部；24—コマンド処理部；25—アクセス制御部；26—大容量不揮発性メモリ I/F部；40—TRM；41—内部不揮発性メモリ；50—

大容量不揮発性メモリ; 5 1—セキュア領域; 5 2—認証領域; 5 3—非認証領域; 6 0—外部CPU; 6 1—携帯電話; 6 2—ROM; 6 3—RAM; 6 4—液晶表示部; 6 5—無線通信部; 6 6—操作ボタン; 6 7—カードI/F部; 6 8—認証回路; 6 9—R/W装置; 7 0—内部バス; 9 1—チャージ用端末; 9 2—チャージサーバ; 9 3—決済サーバ; 9 4—配信サーバ; 9 5—ネットワーク; 6 2 1—コマンド生成プログラム; 6 2 2—認証鍵群を示すものである。

<発明を実施するための最良の形態>

- 10 本発明の実施形態における半導体メモリカード（ここでは「セキュアメモリカード」と呼ぶことにする）は、図1の概念図に示すように、内部不揮発性メモリ4 1を備える耐タンパー性モジュール（tamper resistant module: TRM）4 0と、非認証領域5 3、認証領域5 2及びセキュア領域5 1を備える大容量不揮発性メモリ5 0と、内部不揮発性メモリ4 1及びセキュア領域5 1に対してアクセスする内部CPU 3 0と、電子機器（リード/ライト（R/W）装置）の外部CPU 6 0と通信して認証処理を行い、認証した外部CPU 6 0の認証領域5 2へのアクセスを許可する制御部2 0とを備えている。

- TRM 4 0の不揮発性メモリ4 1は、例えば、1 6バイト単位で消去・書き込みができるEEPROMから成り、また、大容量不揮発性メモリ5 0は、例えば、20 5 1 2バイト等のブロック単位での消去と1バイト単位での書き込みとが可能なフラッシュメモリから成る。

- 外部CPU 6 0は、非認証領域5 3に無条件でアクセスすることができ、また、認証領域5 2には、制御部2 0での認証を済ませた場合にアクセスすることができる。しかし、外部CPU 6 0は、セキュア領域5 1及び内部不揮発性メモリ4 1の存在を知ることができず、これらに直接アクセスすることはできない。

セキュア領域5 1及び内部不揮発性メモリ4 1に対しては、内部CPU 3 0だけがアクセス可能である。セキュア領域5 1と内部不揮発性メモリ4 1との違いは、内部不揮発性メモリ4 1がTRM 4 0に設けられているのに対し、セキュア領域5 1が、耐タンパー性を持たない大容量不揮発性メモリ5 3に設けられてい

る点である。そのため、セキュア領域 5 1 は、内部不揮発性メモリ 4 1 に比べて大きい蓄積容量を持つことができる。その反面、セキュリティレベルは、TRM 4 0 に設けられた内部不揮発性メモリ 4 1 よりも低い。この 4 つの領域のセキュリティレベルは、非認証領域 5 3 が最も低く、認証領域 5 2、セキュア領域 5 1、
5 内部不揮発性メモリ 4 1 の順に高くなっている。

セキュアメモリカード 1 0 の構成の詳細は後述するとして、その使用形態について説明する。

セキュアメモリカードは、例えば、図 3 に示す音楽配信システムなどで使用することができる。このシステムでは、セキュアメモリカード 1 0 が R/W 装置である携帯電話 6 1 に装着される。また、このシステムには、ネットワーク 9 5 を
10 介して音楽を配信する配信サーバ 9 4 と、決済処理を行う決済サーバ 9 3 と、デジタルキャッシュをメモリカード 1 0 にチャージするチャージサーバ 9 2 と、デジタルキャッシュのチャージ用端末 9 1 とが存在している。

携帯電話 6 1 は、図 4 のブロック図に示すように、図 1 の外部 CPU に相当する CPU 6 0 と、認証に使用する認証鍵群 6 2 2 やコマンド生成プログラム 6 2 1 を予め記憶している ROM 6 2 と、CPU 6 0 の作業領域として使用される RAM 6 3 と、表示画面を構成する液晶表示部 6 4 と、ネットワークを介して無線通信を行う無線通信部 6 5 と、ユーザが操作する操作ボタン 6 6 と、セキュアメモリカード 1 0 を内部バス 7 0 に接続するカード I/F 部 6 7 と、セキュアメモリカード 1 0 との相互認証を行う認証回路 6 8 とを備えており、これらの各部が
20 内部バス 7 0 で接続されている。

ユーザは、まず、セキュアメモリカード 1 0 にデジタルキャッシュをチャージする。そのために、ユーザは、セキュアメモリカード 1 0 をチャージ端末 9 1 に装着し、表示された指示に従ってチャージ端末 9 1 を操作する。このとき、チャ
25 ージ端末 9 1 は、セキュアメモリカード 1 0 の内部 CPU 3 0 に入金アプリケーションの起動を要求する。入金アプリケーションを起動した内部 CPU 3 0 は、チャージ端末 9 1 からデジタルキャッシュの入金処理要求を受けると、その要求のコマンドから、データの書き込み先を内部不揮発性メモリ 4 1 と判断し、チャ

ージ端末 9 1 から伝えられた金額を内部不揮発性メモリ 4 1 に書き込む。こうして内部不揮発性メモリ 4 1 にキャッシュ情報が蓄積される。

また、デジタルキャッシュのチャージは、セキュアメモリカード 1 0 を装着した携帯電話 6 1 から、チャージサーバ 9 2 にアクセスして、オンラインで行うこともできる。

次に、ユーザは、携帯電話 6 1 から配信サーバ 9 4 にアクセスし、音楽コンテンツの購入を依頼する。配信サーバ 9 4 は、音楽コンテンツの代金の決済を要求する。これを受けて携帯電話 6 1 の CPU 6 0 は、セキュアメモリカード 1 0 の内部 CPU 3 0 に決済アプリケーションの起動を要求する。決済アプリケーションを起動した内部 CPU 3 0 は、携帯電話 6 1 を認証した後、携帯電話 6 1 から伝えられた支払額を内部不揮発性メモリ 4 1 に記録されたデジタルキャッシュの残額から減算する。これを受けて配信サーバ 9 4 は、電子レシートを携帯端末 6 1 に送信し、携帯端末 6 1 の CPU 6 0 は、この電子レシートの格納要求をセキュアメモリカード 1 0 の内部 CPU 3 0 に送る。内部 CPU 3 0 は、その要求のコマンドから、データの書き込み先をセキュア領域 5 1 と判断して、電子レシートをセキュア領域 5 1 に蓄積する。

なお、決済処理は、内部不揮発性メモリ 4 1 に格納されたクレジット番号を決済サーバ 9 3 に提示して、決済サーバ 9 3 との間で行うこともできる。

決済の終了後、配信サーバ 9 4 は、暗号化された音楽コンテンツと、その復号鍵とを携帯電話 6 1 に送信する。携帯電話 6 1 の CPU 6 0 は、受信データを判断し、コンテンツの復号鍵をセキュアメモリカード 1 0 の認証領域 5 2 に格納し、また、暗号化されたコンテンツをセキュアメモリカード 1 0 の非認証領域 5 3 に格納する。

このように、このシステムでは、セキュアメモリカード 1 0 の TRM 4 0 の内部不揮発性メモリ 4 1 にはキャッシュ情報が格納され、セキュア領域 5 1 には電子レシートが、認証領域 5 2 には復号鍵が、また、非認証領域 5 3 には暗号化されたコンテンツがそれぞれ格納される。

図 2 のブロック図は、セキュアメモリカード 1 0 の構成を示している。セキュアメモリカード 1 0 は、大別して、制御部 2 0 と、大容量不揮発性メモリ 5 0 と、

図１のＴＲＭ４０に相当するＩＣ部１１とで構成される。大容量不揮発性メモリ５０は、非認証領域５３と、認証領域５２と、セキュア領域５１と、これらの領域のアドレス情報が格納されたアドレス情報管理領域５４とを有している。

制御部２０は、Ｒ／Ｗ装置６９との間でデータの授受を行うデータＩ／Ｆ部２１と、Ｒ／Ｗ装置６９との間でコマンドの授受を行うコマンドＩ／Ｆ部２２と、Ｒ／Ｗ装置６９を認証する制御認証部２３と、受け付けたコマンドを解釈してコマンドに応じた処理を行う制御コマンド処理部２４と、大容量不揮発性メモリ５０へのアクセスを制御するとともにＩＣ部１１とのデータの受け渡し窓口となるアクセス制御部２５と、大容量不揮発性メモリ５０との間でデータを受け渡す大容量不揮発性メモリＩ／Ｆ部２６とを備えている。

また、耐タンパー性のＩＣ部１１は、内部不揮発性メモリ４１と、制御部２０との間でデータやコマンドの授受を行うＩ／Ｆ部１２と、コマンドを解釈してコマンドに応じた処理を行うＩＣコマンド処理部１３と、内部不揮発性メモリ４１及びセキュア領域５１にファイル形式で格納されたデータを管理するファイル管理部１４と、Ｒ／Ｗ装置６９を認証し、認証したＲ／Ｗ装置６９に対して内部不揮発性メモリ４１及びセキュア領域５１へのデータアクセスを許可するＩＣ認証部１５と、内部不揮発性メモリ４１及びセキュア領域５１への書き込み／読み出しデータに対して内部不揮発性メモリ４１に格納された鍵を用いて暗号化／復号化を行う暗復号回路１７と、内部不揮発性メモリ４１及びセキュア領域５１の管理を行うメモリ管理部１６と、内部不揮発性メモリ４１へのデータの授受を行う内部不揮発性メモリＩ／Ｆ部１８とを備えている。特許請求の範囲で云うセキュア制御部は、ＩＣ部１１のＩＣコマンド処理部１３、ＩＣ認証部１５、暗復号化回路１７、ファイル管理部１４及びメモリ管理部１６に対応する。

制御部２０の制御コマンド処理部２４は、Ｒ／Ｗ装置６９から受信したコマンドを解釈し、そのコマンドが

- ・大容量不揮発性メモリ５０の認証領域５２または非認証領域５３へのアクセスを要求するものであるか、
- ・認証を要求するものであるか、
- ・ＩＣ部１１による処理を要求するものであるか

を判断し、大容量不揮発性メモリ 50 の認証領域 52 または非認証領域 53 へのアクセスを要求しているときは、アクセス制御部 25 に大容量不揮発性メモリ 50 へのアクセス制御を指示し、IC 部 11 による処理を要求しているときは、アクセス制御部 25 に IC 部 11 へのコマンドの転送を指示し、また、認証を要求しているときは、制御認証部 23 に認証処理を指示する。

認証領域 52 へのアクセスは、その端末に対する制御認証部 23 の認証が済んでいる場合にのみ、受け入れられる。

アクセス制御部 25 は、大容量不揮発性メモリ 50 へのアクセス制御に当たって、大容量不揮発性メモリ 50 のアドレス情報管理領域 54 に記録されたアドレス情報を参照する。端末 (R/W 装置 69) が大容量不揮発性メモリ 50 の論理アドレスを指定してアクセスを求めて来たときは、アドレス情報管理領域 54 の記録から、指定されたアドレスが大容量不揮発性メモリ 50 のいずれの領域に属しているかを判断し、認証領域 52 へのアクセス要求に対しては、認証済み端末に限って許可する。

また、IC 部 11 の IC コマンド処理部 13 は、制御部 20 から送信されたコマンドを解釈し、その処理要求が、

- ・内部不揮発性メモリ 41 へのデータ書き込み/読み出しを要求するものであるか、
 - ・セキュア領域 51 へのデータ書き込み/読み出しを要求するものであるか、
 - ・認証を要求するものであるか、
 - ・その他の処理を要求するものであるか
- を判断する。

IC コマンド処理部 13 は、コマンドがアプリケーションの起動を要求しているときには、内部にそのアプリケーションを起動する。

アプリケーションとは、R/W 装置 69 から受け取ったコマンドの解釈形態であり、アプリケーション起動後に R/W 装置 69 から IC コマンド処理部 13 が受け取ったコマンドは、そのアプリケーションと R/W 装置 69 との間で取り決めた解釈が IC コマンド処理部 13 によって行われる。

アプリケーション起動後に受け取ったコマンドが、認証を要求しているときには、ICコマンド処理部13は、IC認証部15にR/W装置69の認証処理を指示する。

5 また、ICコマンド処理部13は、コマンドが、内部に起動したアプリケーションとR/W装置69との間で取り決めた、内部不揮発性メモリ41へのデータの書き込み/読み出し、または、セキュア領域51へのデータの書き込み/読み出しを要求するコマンドであるときは、IC認証部15において認証処理が済まされているか確認する。

10 認証処理が済まされている場合は、その要求を許可し、その要求が書き込み求であるときは、書き込むデータを、格納先の情報を付してメモリ管理部16に送る。

15 内部不揮発性メモリ41及びセキュア領域51を管理するメモリ管理部16は、書き込むデータを暗復号回路17で暗号化（このとき暗復号回路17は、内部不揮発性メモリ41に格納された暗号鍵を用いて暗号化を行う）した後、内部不揮発性メモリ41に書き込むべきデータを、内部不揮発性メモリI/F部18を介して、内部不揮発性メモリ41に書き込み、書き込み位置の情報をファイル管理部14に伝える。また、セキュア領域51に書き込むべきデータを、大容量不揮発性メモリI/F部26を介して、大容量不揮発性メモリ50のセキュア領域51に書き込み、書き込み位置の情報をファイル管理部14に伝える。

20 ファイル管理部14は、メモリ管理部16から伝えられた情報を基に、内部不揮発性メモリ41及びセキュア領域51に格納されたファイルを管理する。

 また、ICコマンド処理部13は、その要求が読み出し要求であるときは、読み出すべきデータのファイル位置をファイル管理部14に求め、メモリ管理部16にそのファイルの読み出しを要求する。

25 メモリ管理部16は、そのファイルをメモリ管理部16が内部不揮発性メモリ41またはセキュア領域51から読み出すと、暗復号回路17でデータを復号化（このとき暗復号回路17は、内部不揮発性メモリ41に格納された鍵を用いて復号化を行う）して、ICコマンド処理部13に送る。

復号化されたデータは、制御部 20 に送られ、データ I/F 部 21 から R/W 装置 69 に送信される。

ここで、大容量不揮発性メモリ 50 の非認証領域 53、認証領域 52 及びセキュア領域 51、並びに内部不揮発性メモリ 41 への書き込み/読み出し条件を整理すると次のようになる。

- ・非認証領域：無条件でアクセス可能である。非認証領域 53 にアクセスするための通常コマンドでデータの書き込み/読み出しを行うことができる。

- ・認証領域：制御部 20 の制御認証部 23 との認証を済ませることが必要である。制御認証部 23 が認証することによって認証領域 52 の論理アドレスを用いてアクセスすることが可能となる。

- ・セキュア領域：IC 部 11 の IC 認証部 15 (= IC 部アプリケーション) との認証を済ませることが必要である。IC 部アプリケーションと端末との間で取り決めたコマンドによりデータの書き込み/読み出しが可能になる (または IC 部アプリケーションの処理の一部としてデータの書き込み/読み出しが可能になる)。端末からはセキュア領域を見ることができず、端末は、セキュア領域の論理アドレスを用いてアクセスすることはできない。

- ・内部不揮発性メモリ：セキュア領域の書き込み/読み出し条件と全く同じである。なお、セキュア領域にアクセスするための認証と内部不揮発性メモリにアクセスするための認証とを異なるものとしてもよい。

図 8 は、大容量不揮発性メモリ 50 の内部構造を示している。ここでは、大容量不揮発性メモリ 50 の物理アドレス上の配置が、非認証領域 53 は 0000~(XXXX-1)、認証領域 52 は XXXX~(ZZZZ-1)、セキュア領域 51 は ZZZZ~(YYYY) の場合を示している。セキュア領域 51 と認証領域 52 との境界を示す第 1 アドレス情報は ZZZZ であり、認証領域 52 と非認証領域 53 との境界を示す第 2 アドレス情報は XXXX である。また、非認証領域 53 のサイズは XXXX、認証領域 52 のサイズは ZZZZ-XXXX、セキュア領域 51 のサイズは YYYY-ZZZZ+1 である。

図 9 は、各領域の物理アドレスと論理アドレスとの対応関係を表す「論理 - 物理アドレス変換テーブル」を示している。非認証領域 53 の論理アドレスは

0000～(XXXX-1)であり、認証領域 5 2 の論理アドレスは 0000～(ZZZZ-XXXX-1)、セキュア領域 5 1 の論理アドレスは 0000～(YYYY-ZZZZ)である。

アドレス情報管理領域 5 4 には、第 1 アドレス情報、第 2 アドレス情報、及び、各領域の論理 - 物理アドレス変換テーブルが保持されている。非認証領域 5 3、
5 認証領域 5 2、及びセキュア領域 5 1 のいずれについても、割り当てられた論理アドレスの境界を越えて論理アドレスを指定することはできないが、各領域の境界を移動して、各領域を拡張または縮小することはできる。

セキュア領域 5 1 の拡張／縮小は、第 1 アドレス情報を変更することによって実現できる。図 9 の論理 - 物理アドレス変換テーブルでは、非認証領域 5 3 及び
10 認証領域 5 2 における論理アドレスの順番を物理アドレスの順序の正順とし、セキュア領域 5 1 における論理アドレスの順番を物理アドレスの順序の逆順としているので、認証領域 5 2 とセキュア領域 5 1 との境界を変更したとき、ともに論理ブロックの末尾アドレスの側だけを修正すれば足りるので、境界変更に伴うテーブルの書き換え負担が少なくなり、高速での処理が可能になる。

15 この境界変更の手順については後述する。

次に、このセキュアメモ리카ードでのデータの格納手順について説明する。

図 5 及び図 6 は、セキュアメモ리카ードを装着した端末から配信サーバにコンテンツ購入を依頼し、代金の決済処理を行い、その電子レシートをセキュア領域に、暗号化されたコンテンツを非認証領域に、また、コンテンツの復号鍵を認証
20 領域に格納するまでの手順を示している。

図 5 に示すように、端末は配信サーバにコンテンツ購入を依頼する (1)。配信サーバは、コンテンツの代金の決済を要求する (2)。端末は、セキュアメモ리카ード 10 の IC 部 11 に決済アプリケーションの起動を要求するコマンドを送信する (3)。制御部 20 の制御コマンド処理部 24 は、このコマンドを IC
25 部に対するコマンドであると認識して、IC 部 11 に送信する (4)。IC 部 11 は、決済アプリケーションを起動して IC 認証部 15 を立ち上げ、応答を端末に返す (5)、(6)。端末は、セキュアメモ리카ード 10 に認証要求コマンドを送り (7)、制御部 20 の制御コマンド処理部 24 は、このコマンドを IC 部に対するコマンドであると認識して、IC 部 11 に送信する (8)。IC 認証部

15は、端末（または配信サーバ）を認証し、認証結果を応答する（9）、（10）。認証が済んだ端末は、セキュアメモリカード10に支払額を示し、決済要求のコマンドを送信する（11）。制御部20の制御コマンド処理部24は、このコマンドをIC部に対するコマンドであると認識して、IC部11に送信する（12）。IC認証部15は、「決済要求」というコマンドにより内部不揮発性メモリ41に書き込むデータであることを判断し、内部不揮発性メモリ41に記録された残高を、支払額を減算した額に書き換える処理を行い、処理終了を応答する（13）、（14）（なお、端末が（9）の認証を済ませていない状態での決済要求は拒否される）。

10 端末は、配信サーバに応答を返す（15）。配信サーバは電子レシートを端末に送信する（16）。端末は、セキュアメモリカード10に電子レシートの格納要求コマンドを送信する（17）。制御部20の制御コマンド処理部24は、このコマンドをIC部に対するコマンドであると認識して、IC部11に送信する。IC認証部15は、「電子レシート格納要求」というコマンドによりセキュア領域51に格納すべきデータであると判断し、電子レシートを暗復号回路17で暗号化した後、セキュア領域51に格納する（18）（なお、端末が（9）の認証を済ませていない状態での電子レシート格納要求は拒否される）。

15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1089 1090 1091 1092 1093 1094 1095 1096 1097 1098 1099 1100 1101 1102 1103 1104 1105 1106 1107 1108 1109 1110 1111 1112 1113 1114 1115 1116 1117 1118 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1189 1190 1191 1192 1193 1194 1195 1196 1197 1198 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1210 1211 1212 1213 1214 1215 1216 1217 1218 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1290 1291 1292 1293 1294 1295 1296 1297 1298 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1389 1390 1391 1392 1393 1394 1395 1396 1397 1398 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1410 1411 1412 1413 1414 1415 1416 1417 1418 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1489 1490 1491 1492 1493 1494 1495 1496 1497 1498 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1510 1511 1512 1513 1514 1515 1516 1517 1518 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1589 1590 1591 1592 1593 1594 1595 1596 1597 1598 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1610 1611 1612 1613 1614 1615 1616 1617 1618 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1689 1690 1691 1692 1693 1694 1695 1696 1697 1698 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1710 1711 1712 1713 1714 1715 1716 1717 1718 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1789 1790 1791 1792 1793 1794 1795 1796 1797 1798 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1810 1811 1812 1813 1814 1815 1816 1817 1818 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1889 1890 1891 1892 1893 1894 1895 1896 1897 1898 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1910 1911 1912 1913 1914 1915 1916 1917 1918 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1950 1951 1952 1953 1954 1955 1956 1957 1958 1959 1960 1961 1962 1963 1964 1965 1966 1967 1968 1969 1970 1971 1972 1973 1974 1975 1976 1977 1978 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2150 2151 2152 2153 2154 2155 2156 2157 2158 2159 2160 2161 2162 2163 2164 2165 2166 2167 2168 2169 2170 2171 2172 2173 2174 2175 2176 2177 2178 2179 2180 2181 2182 2183 2184 2185 2186 2187 2188 2189 2190 2191 2192 2193 2194 2195 2196 2197 2198 2199 2200 2201 2202 2203 2204 2205 2206 2207 2208 2209 2210 2211 2212 2213 2214 2215 2216 2217 2218 2219 2220 2221 2222 2223 2224 2225 2226 2227 2228 2229 2230 2231 2232 2233 2234 2235 2236 2237 2238 2239 2240 2241 2242 2243 2244 2245 2246 2247 2248 2249 2250 2251 2252 2253 2254 2255 2256 2257 2258 2259 2260 2261 2262 2263 2264 2265 2266 2267 2268 2269 2270 2271 2272 2273 2274 2275 2276 2277 2278 2279 2280 2281 2282 2283 2284 2285 2286 2287 2288 2289 2290 2291 2292 2293 2294 2295 2296 2297 2298 2299 2300 2301 2302 2303 2304 2305 2306 2307 2308 2309 2310 2311 2312 2313 2314 2315 2316 2317 2318 2319 2320 2321 2322 2323 2324 2325 2326 2327 2328 2329 2330 2331 2332 2333 2334 2335 2336 2337 2338 2339 2340 2341 2342 2343 2344 2345 2346 2347 2348 2349 2350 2351 2352 2353 2354 2355 2356 2357 2358 2359 2360 2361 2362 2363 2364 2365 2366 2367 2368 2369 2370 2371 2372 2373 2374 2375 2376 2377 2378 2379 2380 2381 2382 2383 2384 2385 2386 2387 2388 2389 2390 2391 2392 2393 2394 2395 2396 2397 2398 2399 2400 2401 2402 2403 2404 2405 2406 2407 2408 2409 2410 2411 2412 2413 2414 2415 2416 2417 2418 2419 2420 2421 2422 2423 2424 2425 2426 2427 2428 2429 2430 2431 2432 2433 2434 2435 2436 2437 2438 2439 2440 2441 2442 2443 2444 2445 2446 2447 2448 2449 2450 2451 2452 2453 2454 2455 2456 2457 2458 2459 2460 2461 2462 2463 2464 2465 2466 2467 2468 2469 2470 2471 2472 2473 2474 2475 2476 2477 2478 2479 2480 2481 2482 2483 2484 2485 2486 2487 2488 2489 2490 2491 2492 2493 2494 2495 2496 2497 2498 2499 2500 2501 2502 2503 2504 2505 2506 2507 2508 2509 2510 2511 2512 2513 2514 2515 2516 2517 2518 2519 2520 2521 2522 2523 2524 2525 2526 2527 2528 2529 2530 2531 2532 2533 2534 2535 2536 2537 2538 2539 2540 2541 2542 2543 2544 2545 2546 2547 2548 2549 2550 2551 2552 2553 2554 2555 2556 2557 2558 2559 2560 2561 2562 2563 2564 2565 2566 2567 2568 2569 2570 2571 2572 2573 2574 2575 2576 2577 2578 2579 2580 2581 2582 2583 2584 2585 2586 2587 2588 2589 2590 2591 2592 2593 2594 25

ンツ鍵の書き込み要求を出す（２５）。制御部２０のアクセス制御部２５は、端末の認証が済んでいるため、認証領域５２へのアクセスを許可し、認証領域５２にコンテンツ鍵が書き込まれる。書き込み終了の応答があると（２６）、端末は、暗号化されたコンテンツを非認証領域５３へ書き込むべきことを判断し、セキュアメモリカード１０に非認証領域５３へのコンテンツの書き込みを要求する（２７）。暗号化されたコンテンツが非認証領域５３に書き込まれ、その応答が端末に返ると（２８）、端末は配信サーバに完了通知を送信する（２９）。

こうして、電子レシートが暗号化してセキュア領域５１に、コンテンツ鍵が認証領域５２に、暗号化されたコンテンツが非認証領域５３に、それぞれ書き込まれる。

なお、図５の手順中、内部不揮発性メモリ４１に記録された残高を、支払額を減算した額に書き換えたとき（１３）、図７に示すように、その支払額をセキュア領域５１に書き込むようにしても良い（１３'）。こうすることで決済ログをセキュア領域５１に記録することができる。

また、決済アプリケーションによる認証（３）を行う前、または後に、利用者を確認するための暗証番号照合を行うようにしてもよい。

次に、大容量不揮発性メモリ５０における各領域間の境界変更の手順について説明する。ここでは、図８の第１アドレス情報を変更してセキュア領域５１を拡張または縮小する場合を示す。

この境界変更は、セキュアメモリカード１０を装着した端末からの要求で行われる。

（１）端末は、セキュアメモリカード１０に対して、境界変更アプリケーションの起動を要求し、このアプリケーションを起動したセキュアメモリカード１０のＩＣ部１１は、ＩＣコマンド処理部１３及びＩＣ認証部１５を立ち上げる。端末は、ＩＣ部１１に対して認証を要求し、ＩＣ認証部１５は、端末を認証する。なお、この認証は、内部不揮発性メモリ４１やセキュア領域５１へのアクセスに要する認証とは別の認証とし、一部の特定端末のみがセキュア領域５１の拡張／縮小を行うことができるようにしても良い。

(2) 認証を受けた端末は、IC部アプリケーション(ICコマンド処理部13)に対して変更後の第1アドレス情報(新たなZZZZ)を通知する。

(3) ICコマンド処理部13は、メモリ管理部16に新たなZZZZを伝えてセキュア領域51の境界変更を指示する。メモリ管理部16は、ZZZZの値に対応するようにセキュア領域51と認証領域52との論理-物理アドレス変換テーブルを修正し、アドレス情報管理領域54に、新たなZZZZの値と、修正した論理-物理アドレス変換テーブルとを格納する。このとき、図9のセキュア領域及び認証領域のテーブル上で、共に論理ブロックの末尾アドレスの側だけが修正される。

10 (4) メモリ管理部16は、セキュア領域51を拡張した場合には、新たにセキュア領域となった部分のデータを消去し、セキュア領域51を縮小した場合には、新たに認証領域52となった部分のデータを消去する。このとき、セキュア領域、及び/または、認証領域のすべてのデータを消去してもよい。

(5) ICコマンド処理部13は、端末に境界変更完了を通知する。

15 また、このとき、IC部の要求に基づいて、セキュアメモ리카ード10の制御部20が、境界変更の処理を行うようにしてもよい。この場合の手順は次のようになる。

(1) 前記(1)と同様に、端末がIC認証部15の認証を受ける。

20 (1') 端末は、セキュアメモ리카ード10の制御部20に対して認証を要求し、制御コマンド処理部24の指示により、制御認証部23が認証領域のサイズ変更を許可するための認証を行う。

(2) 前記(2)と同様に、端末が、ICコマンド処理部13に対して変更後の第1アドレス情報(新たなZZZZ)を通知する。

25 (3) ICコマンド処理部13は、アクセス制御部25を経由して、制御部コマンド処理部24に境界アドレス変更を要求する。

(3') 制御部コマンド処理部24は、アドレス情報管理領域54にZZZZの値を保存し、あわせて、ZZZZの値に対応するようにセキュア領域と認証領域との論理-物理アドレス変換テーブルを修正する。(ただし、(1')の認証が行われ

ていない場合は境界アドレスの変更を拒否し、拒否したことを I C コマンド処理部 1 3 に通知する)

(4) 制御部コマンド処理部 2 4 は、セキュア領域を拡張した場合に、新たにセキュア領域となった部分のデータを消去し、セキュア領域を縮小した場合に、新たに認証領域となった部分のデータを消去する。また、セキュア領域、及び／または、認証領域のすべてのデータを消去してもよい。

(5) 制御部コマンド処理部 2 4 は、I C コマンド処理部 1 3 に境界変更完了を伝え、I C コマンド処理部 1 3 は、端末に境界変更完了を通知する(ただし、

(3') において境界アドレスの変更が拒否された場合は、端末に境界変更の拒否を通知する)。

また、認証領域の拡張／縮小は、認証領域と非認証領域との境界の第 2 アドレス情報を変更することにより行う。この場合の手順は次のようになる。

(1) 端末は、セキュアメモ리카ード 1 0 の制御部 2 0 に対して認証を要求し、制御コマンド処理部 2 4 の指示により、制御認証部 2 3 が認証領域のサイズ変更を許可するための認証を行う。

(2) 認証を受けた端末は、制御部 2 0 に対して変更後の第 2 アドレス情報(新たな XXXX)を通知する。

(3) 制御部コマンド処理部 2 4 は、アドレス情報管理領域 5 4 に XXXX の値を保存し、あわせて、XXXX の値に対応するように非認証領域と認証領域との論理—物理アドレス変換テーブルを修正する(ただし、(1)の認証が行われていない場合は境界アドレスの変更を拒否し、拒否したことを端末に通知する)。

(4) 制御部コマンド処理部 2 4 は、認証領域を拡張した場合に、新たに認証領域となった部分のデータを消去し、認証領域を縮小した場合に、新たに非認証領域となった部分のデータを消去する。また、非認証領域、及び／または、認証領域のすべてのデータを消去してもよい。

(5) 制御部コマンド処理部 2 4 は、端末に境界変更完了を通知する。

なお、この場合、図 1 0 に示すように、論理—物理アドレス変換テーブルの非認証領域 5 3 における論理アドレスの順番が物理アドレスの順序の正順であり、認証領域 5 2 における論理アドレスの順番が物理アドレスの順序の逆順であると、

境界変更の際に、ともに論理ブロックの末尾アドレスの側だけを修正すれば足りるので、境界変更に伴うテーブルの書き換え負担が少なくなり、高速での処理が可能になる。

非認証領域の拡張／縮小は、認証領域の拡張／縮小処理により実現できる。

- 5 また、大容量不揮発性メモリ 50 には、図 11 に示すように、セキュア領域 51、非認証領域 53、認証領域 52 の順に各領域を配置しても良い。図 12 には、このときの論理－物理アドレス変換テーブルの一例を示している。

- また、この場合、セキュア領域 51 を端末から見えない領域とするため、または、セキュア領域を持たないメモリカードとの互換性を保つために、図 11 に示すように、実際の境界アドレスとは異なる「端末みなしアドレス」を設けるよう
10 にしてもよい。この端末みなしアドレスでは、セキュア領域を省いて、非認証領域 53 の先頭のみなし物理アドレスを 0000 とし（実際は XXXX'）、非認証領域 53 と認証領域 52 との境界のみなし物理アドレスを ZZZZ'（実際は ZZZZ'）、認証領域
15 端末のみなし物理アドレスを YYYY'（実際は YYYY'）とする。端末は境界アドレスを ZZZZ' と認識し、領域の拡張／縮小を要求する際に、この ZZZZ' の変更を要求するが、制御コマンド処理部は、ZZZZ' と ZZZZ' との関係を認識し、実際の物理アドレス ZZZZ' に置き換えて、境界の変更を行う。

- なお、本発明の実施形態では、大容量不揮発性メモリ 50 に、記憶領域として、非認証領域、認証領域及びセキュア領域の 3 領域を設ける場合について説明したが、
20 大容量不揮発性メモリ 50 に、セキュア領域の他に、非認証領域または認証領域の一方だけを通常領域として設けるようにしても良い。

 また、ここでは主に、セキュアメモリカードの IC 部に決済用アプリケーションを搭載する場合について説明したが、その他、署名を生成するアプリケーションを搭載することも可能である。

- 25 この場合、データのセキュア領域への書き込み時に書き込みデータのハッシュ値を計算し、それを IC 部の内部不揮発性メモリに格納し、ハッシュ値に対して電子署名を生成する。データのセキュア領域からの読み出し時（復号化後）には、再度ハッシュ値を計算し、書き込み時に IC 部の内部不揮発性メモリに格納したハッシュ値と比較することでデータの欠損、改ざんなどを検知する。

こうした機能を搭載することで、このセキュアメモリカードは、決済する際に利用することもできるし、何らかのデータに電子署名を付与する際にも利用することができる。

5 また、このセキュアメモリカードを用いるR/W装置として、デジタルコンテンツ配信サービス用アプリケーションを搭載し、決済機能と、コンテンツのダウンロード及びメモリカードへの格納機能とを持つ場合について説明したが、セキュアメモリカードを活用する上で、R/W装置には次の機能を持つことが求められる。

10 ・セキュアメモリカードの通常領域を読み書きするためのコマンドを生成することができる。

・セキュアメモリカードのIC部に処理を要求するためのICコマンドを生成することができる。

15 ・IC部アプリケーション（IC認証部）と認証を行うための認証鍵を取得して、それを用いて認証に必要なデータ（IC部アプリケーションから提供された乱数に対して暗号または署名を施したデータ）を生成することができる。

また、セキュアメモリカードが通常領域として、非認証領域及び認証領域を有する場合には、これに加えて、

・認証領域を読み書きするためのコマンドを生成することができる。

20 ・セキュアメモリカードの制御認証部と認証を行うための認証鍵を取得して、それを用いて認証に必要なデータを生成することができる。
ことが求められる。

なお、認証鍵の取得は、R/W装置（電子機器）が認証鍵をROMなどで保持している場合には、そこから入手する。また、電子機器が認証鍵を保持していない場合には、外部の機器（サーバ、リムーバブルメディア等）から受信する。

25 また、本発明のセキュアメモリカード10が有する大容量不揮発性メモリ50を、他の記憶メディア、例えば、ハードディスク、光ディスク、光磁気ディスク等の不揮発メディアに置き換えても、本発明と同様、大容量・高セキュリティなメモリデバイスが実現されることは言うまでもない。

また、本発明のセキュアメモリカード10は、電子機器に対して着脱可能である必要は無く、例えば電子機器にICチップを埋め込んだ一体型機器などのように、電子機器と固定的に接続されていても良い。また、カード／チップのような形状である必要もなく、ディスクやテープなどの形態であっても一向に構わない。

- 5 また、本発明の電子機器（60、61、69）は、固定設置端末、携帯端末、携帯電話など、メモリデバイスが接続できるものであればどのようなものでも一向に構わない。

- つまり、本発明の実施形態で説明したもの以外でも、携帯電話にICチップを埋め込んだもの、固定設置端末にハードディスクを装着したようなもの等、その
10 用途に応じて様々な形態が考えられる。

本発明を詳細に、また、特定の実施態様を参照して説明したが、本発明の精神と範囲を逸脱することなく、様々な変更や修正を加えることができることは、当業者にとって明らかである。

- 15 本出願は、2002年12月16日出願の日本特許出願（特願2002-363597号）に基づくものであり、その内容は、ここに参照して取り込まれる。

<産業上の利用可能性>

- 20 以上の説明から明らかなように、本発明のメモリデバイスは、セキュリティレベルがICカードと同等であって、記憶容量がICカードに比べて遥かに大きいメモリ領域を持つことができる。

- また、このメモリデバイスは、複数のセキュリティレベルのメモリ領域を備えており、一つのデバイスでデジタルキャッシュや音楽配信等の多用なサービスに対応することができる。また、この複数のメモリ領域の大きさは、必要に応じて
25 変更することができる。

また、本発明の電子機器（R/W装置）は、このメモリデバイスを活用して、多様なサービスの実現を図ることができる。

請求の範囲

1. 電子機器に固定的にまたは着脱可能に接続されるメモリデバイスであって、

前記電子機器からアクセスすることが可能な通常領域と、前記電子機器から直接アクセスすることができないセキュア領域とを有する、非耐タンパー性の第1のメモリと、

前記電子機器から直接アクセスすることができない耐タンパー性の第2のメモリと、

前記第2のメモリへのアクセスを管理するセキュア制御部と、
を備えており、

前記電子機器から前記第1のメモリのセキュア領域へのアクセスは、前記セキュア制御部を介してのみ可能であること、

を特徴とするメモリデバイス。

2. 請求項1に記載のメモリデバイスであって、

前記セキュア制御部は、前記セキュア制御部が認証した電子機器のコマンドを受けて前記セキュア領域または第2のメモリにアクセスし、データの書き込みまたは読み出しを行うこと、

を特徴とするメモリデバイス。

3. 請求項1または請求項2に記載のメモリデバイスであって、

前記第2のメモリには、暗号鍵が格納されており、

前記セキュア制御部は、前記セキュア領域に書き込むデータを前記暗号鍵を用いて暗号化して書き込み、且つ、前記セキュア領域から読み出したデータを前記暗号鍵を用いて復号化すること、

を特徴とするメモリデバイス。

4 請求項1から請求項3のいずれかに記載のメモリデバイスであって、

前記セキュア制御部は、前記セキュア領域に書き込むデータのハッシュ値を計算して、前記ハッシュ値を前記第2のメモリに格納し、前記セキュア領域から読み出したデータのハッシュ値を計算して、前記第2のメモリに格納したハッシュ値と照合すること、

を特徴とするメモリデバイス。

5 請求項1に記載のメモリデバイスであって、

前記第1のメモリの通常領域が、メモリデバイスを制御する全体制御部によって認証された電子機器のみがアクセスできる認証領域と、認証を受けない電子機器でもアクセスできる非認証領域とを含むこと、

を特徴とするメモリデバイス。

6 請求項1から請求項5のいずれかに記載のメモリデバイスであって、

前記通常領域と前記セキュア領域との境界を示す境界アドレス情報と、前記通常領域及びセキュア領域の各々における論理アドレスと物理アドレスとの関係を記述した論理－物理アドレス変換テーブルとが、前記第1のメモリのアドレス情報として管理されていること、

を特徴とするメモリデバイス。

7. 請求項6に記載のメモリデバイスであって、

前記第1のメモリのアドレス情報に、前記認証領域と前記非認証領域との境界を示す境界アドレス情報と、前記認証領域及び非認証領域の各々における論理－物理アドレス変換テーブルとが含まれていること、

を特徴とするメモリデバイス。

8. 請求項6または請求項7に記載のメモリデバイスであって、

前記境界アドレス情報及び論理－物理アドレス変換テーブルが、前記第1のメモリのアドレス情報管理領域に記録されていること、

を特徴とするメモリデバイス。

9 請求項6に記載のメモリデバイスであって、
前記境界アドレス情報で表された前記通常領域と前記セキュア領域との境界が、
前記セキュア制御部の認証を受けた電子機器のコマンドで変更されること、
を特徴とするメモリデバイス。

10 請求項7に記載のメモリデバイスであって、
前記境界アドレス情報で表された前記認証領域と前記非認証領域との境界が、
前記全体制御部の認証を受けた電子機器のコマンドで変更されること、
を特徴とするメモリデバイス。

11 請求項10に記載のメモリデバイスであって、
前記認証領域と前記非認証領域との境界の境界アドレス情報が、実境界アドレスと、
セキュア領域を除いて設定したみなし境界アドレスとから成り、
前記全体制御部の認証を受けた電子機器のコマンドによって指定された前記みなし境界アドレスに基づいて、前記実境界アドレスが変更されること、
を特徴とするメモリデバイス。

12 メモリ領域として第1領域、第2領域、及び第3領域を有するメモリデバイスに対して、アクセスを行う電子機器であって、
前記電子機器は、メモリデバイスへのアクセス要求を受けると、
メモリデバイスの非耐タンパー性のメモリ領域である前記第1領域に、メモリデバイスへのアクセスを制御するメモリデバイスの全体制御部を介してアクセスし、

前記全体制御部、並びに、第2領域及び第3領域へのアクセスを制御するメモリデバイスのセキュア制御部の認証を受けた後、第1領域以外の非耐タンパー性のメモリ領域である前記第2領域には、前記セキュア制御部を介してアクセスし、

前記セキュア制御部との認証を経た後、メモリデバイスの耐タンパー性のメモリ領域である前記第 3 領域には、前記全体制御部及び前記セキュア制御部を介してアクセスする、

ことを特徴とする電子機器。

1 3. 請求項 1 2 に記載の電子機器であって、

第 1 領域に対するデータの書き込みまたは読み出しのコマンドを生成する第 1 のコマンド生成手段と、

セキュア制御部に処理を要求するコマンドを生成する第 2 のコマンド生成手段と、

前記セキュア制御部との認証に用いる認証鍵を取得し、前記セキュア制御部との認証処理を行う第 1 の認証処理手段と、

を備える電子機器。

1 4. 請求項 1 2 または請求項 1 3 に記載の電子機器であって、

第 1 領域の一部の領域である非認証領域には、全体制御部との認証を経ることなくアクセスを行い、非認証領域以外で、第 1 領域の一部または全部の領域である認証領域には、全体制御部との認証を経た後にアクセスを行う、

ことを特徴とする電子機器。

1 5. 請求項 1 4 に記載の電子機器であって、

認証領域に対するデータの書き込みまたは読み出しのコマンドを生成する第 3 のコマンド生成手段と、

全体制御部との認証に用いる認証鍵を取得し、前記全体制御部との認証処理を行う第 2 の認証処理手段と、

を備える電子機器。

図 1

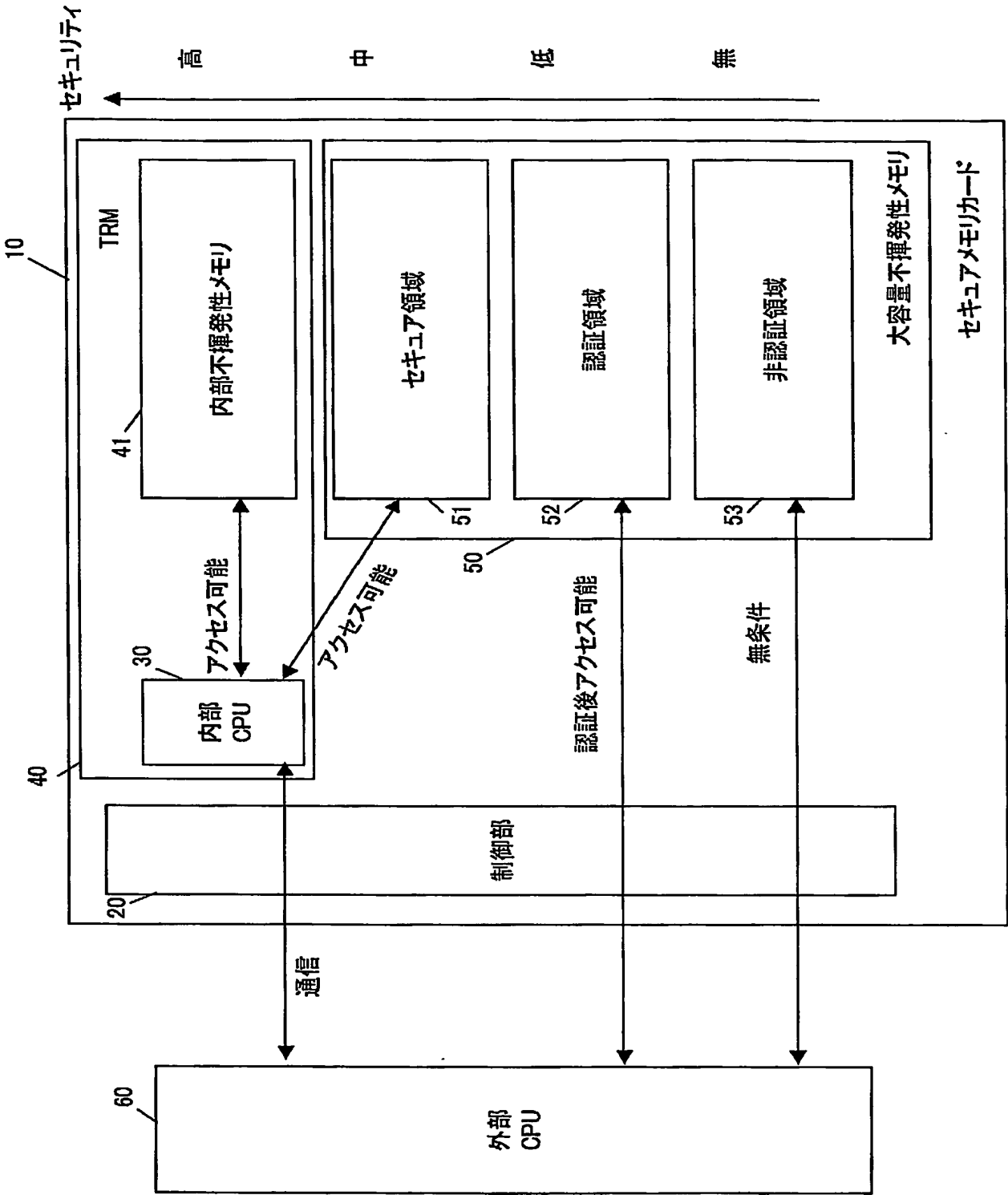


図 2

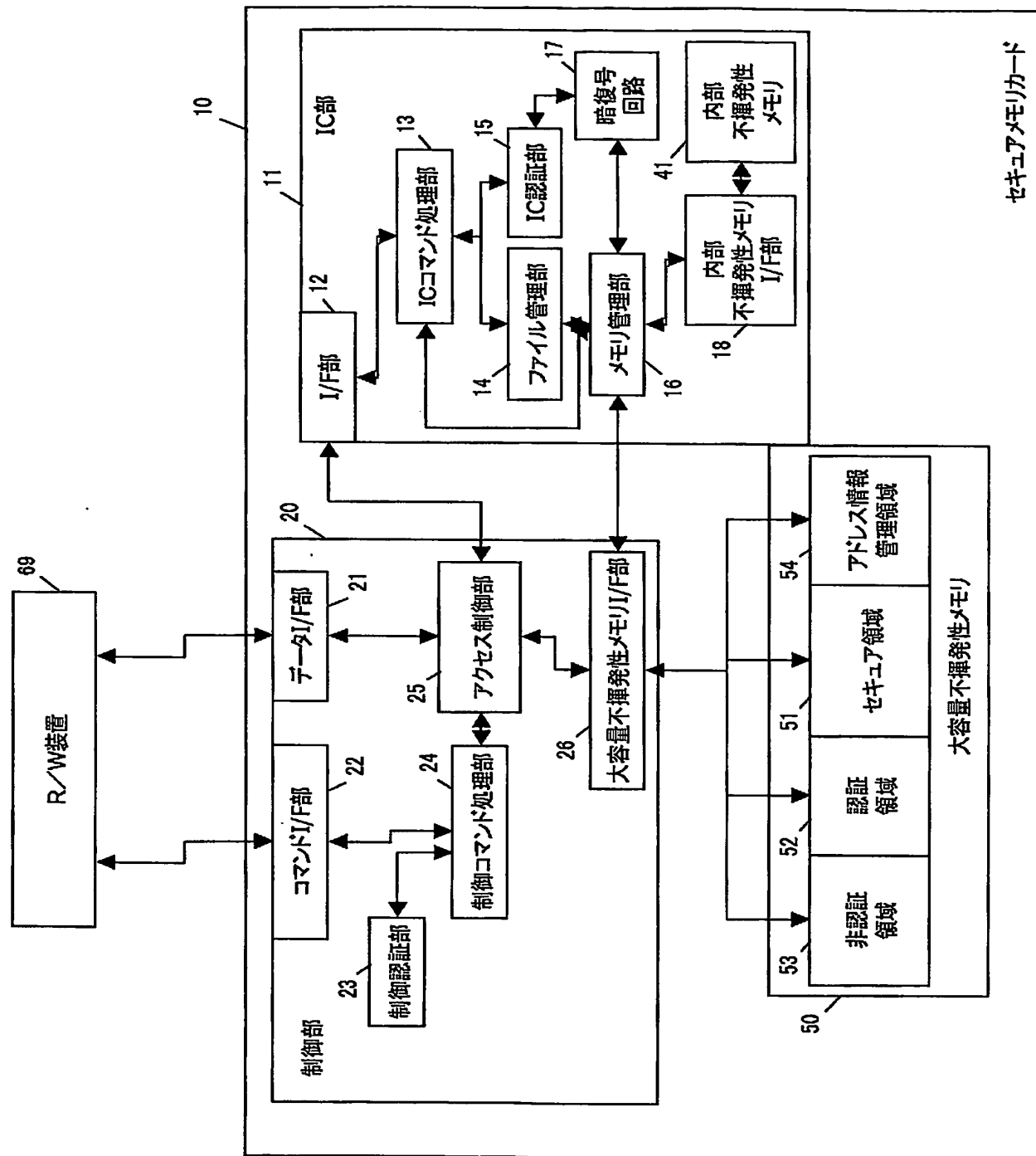


図 3

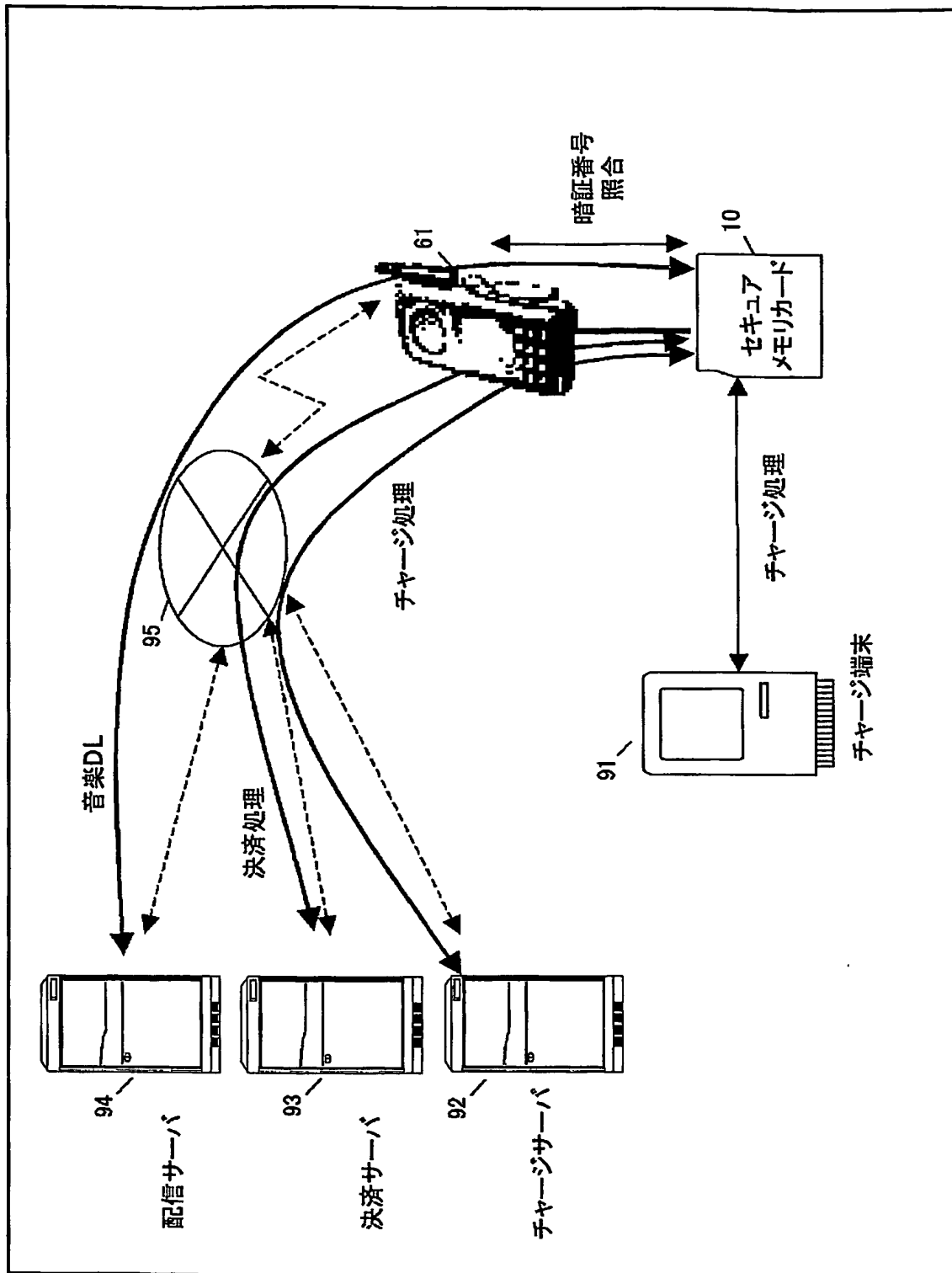


図 4

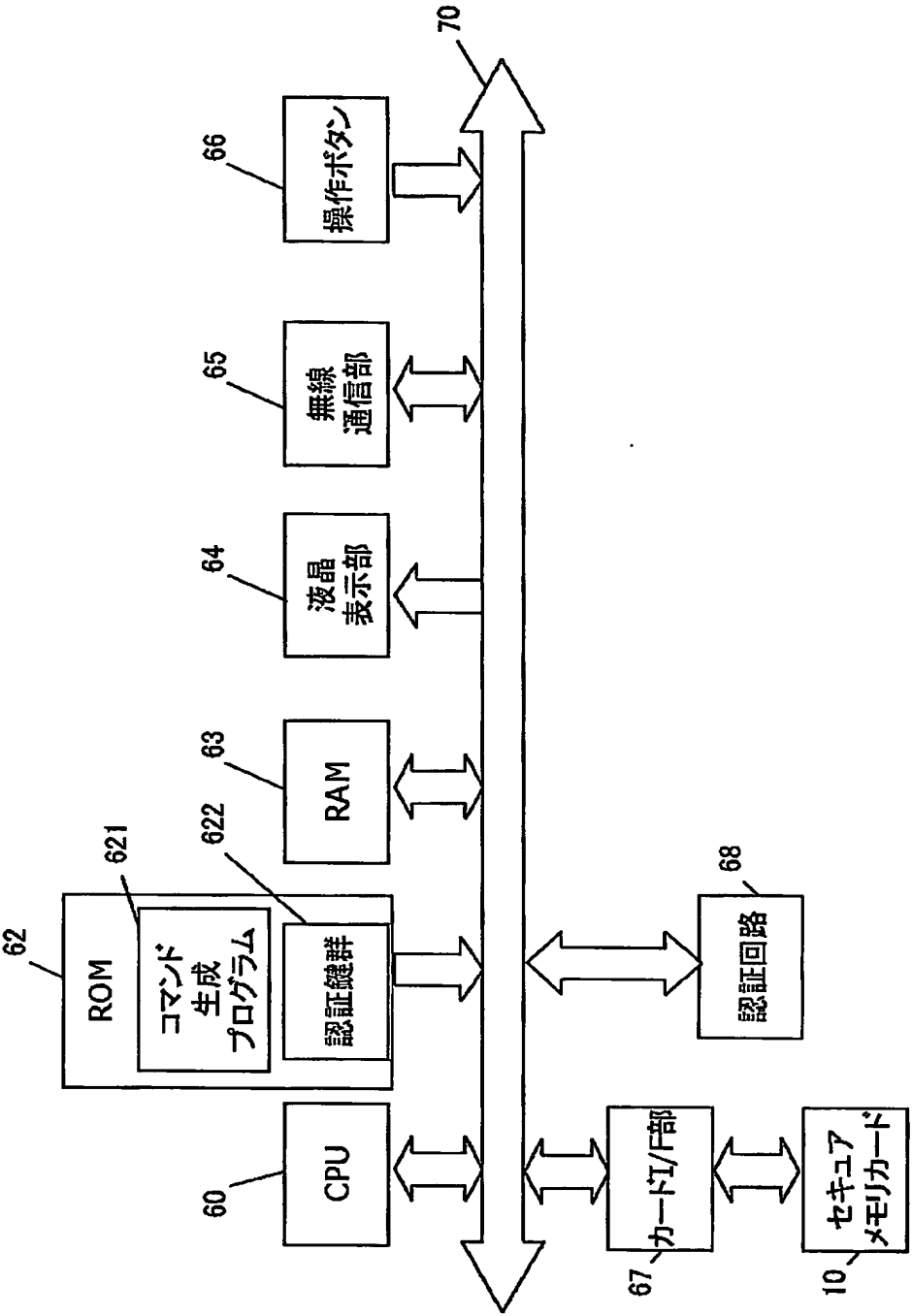


図 5

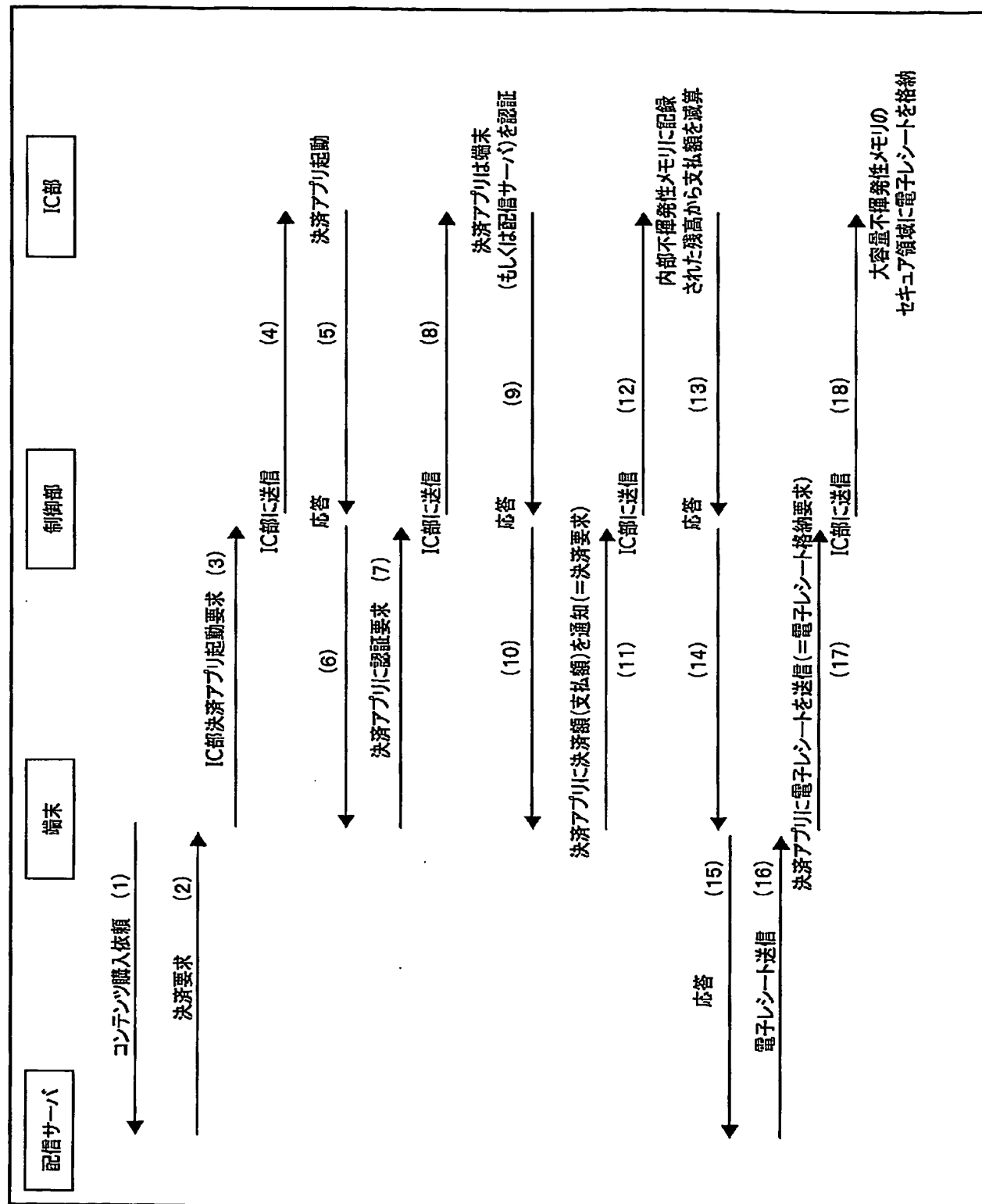


図 6

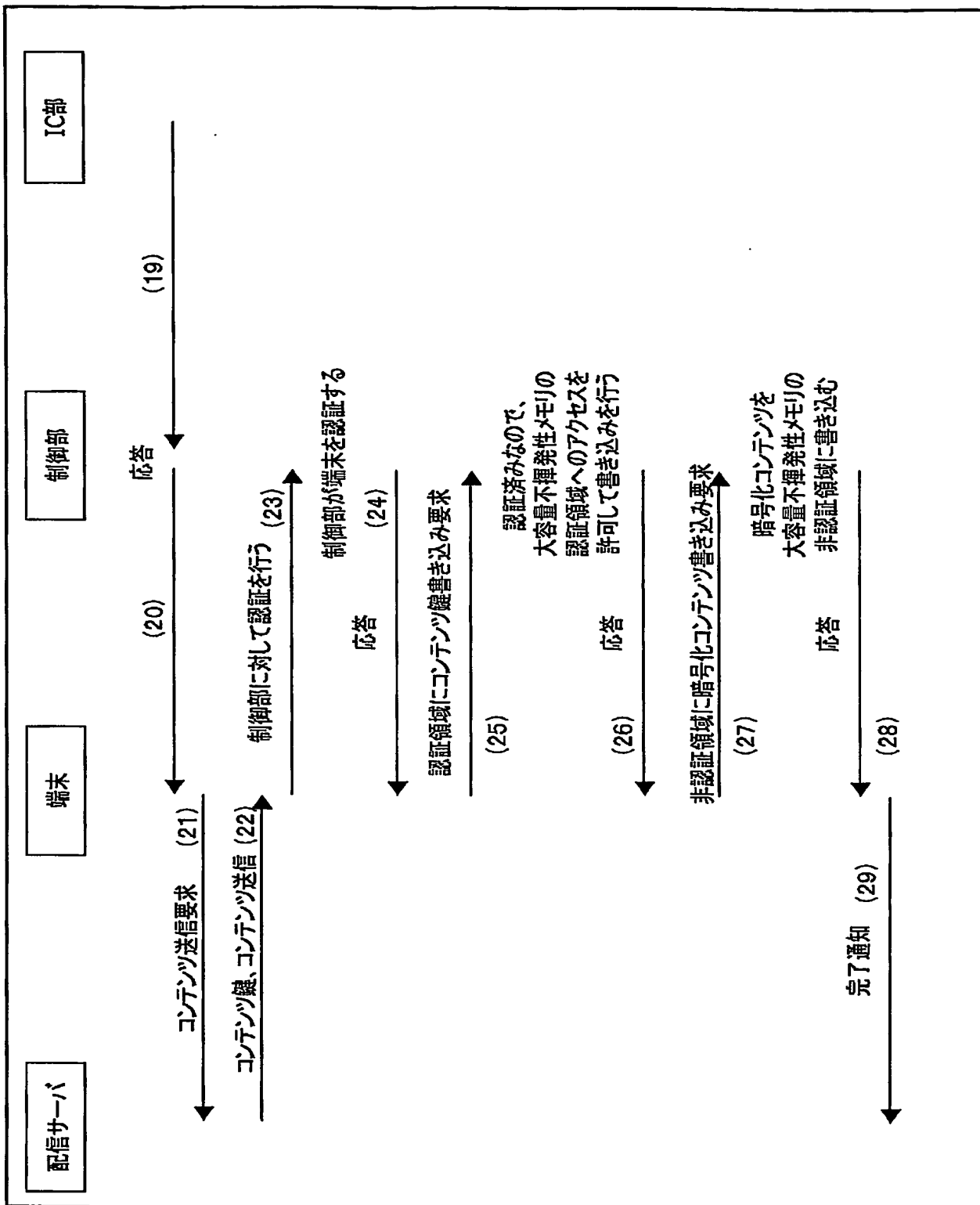


図 7

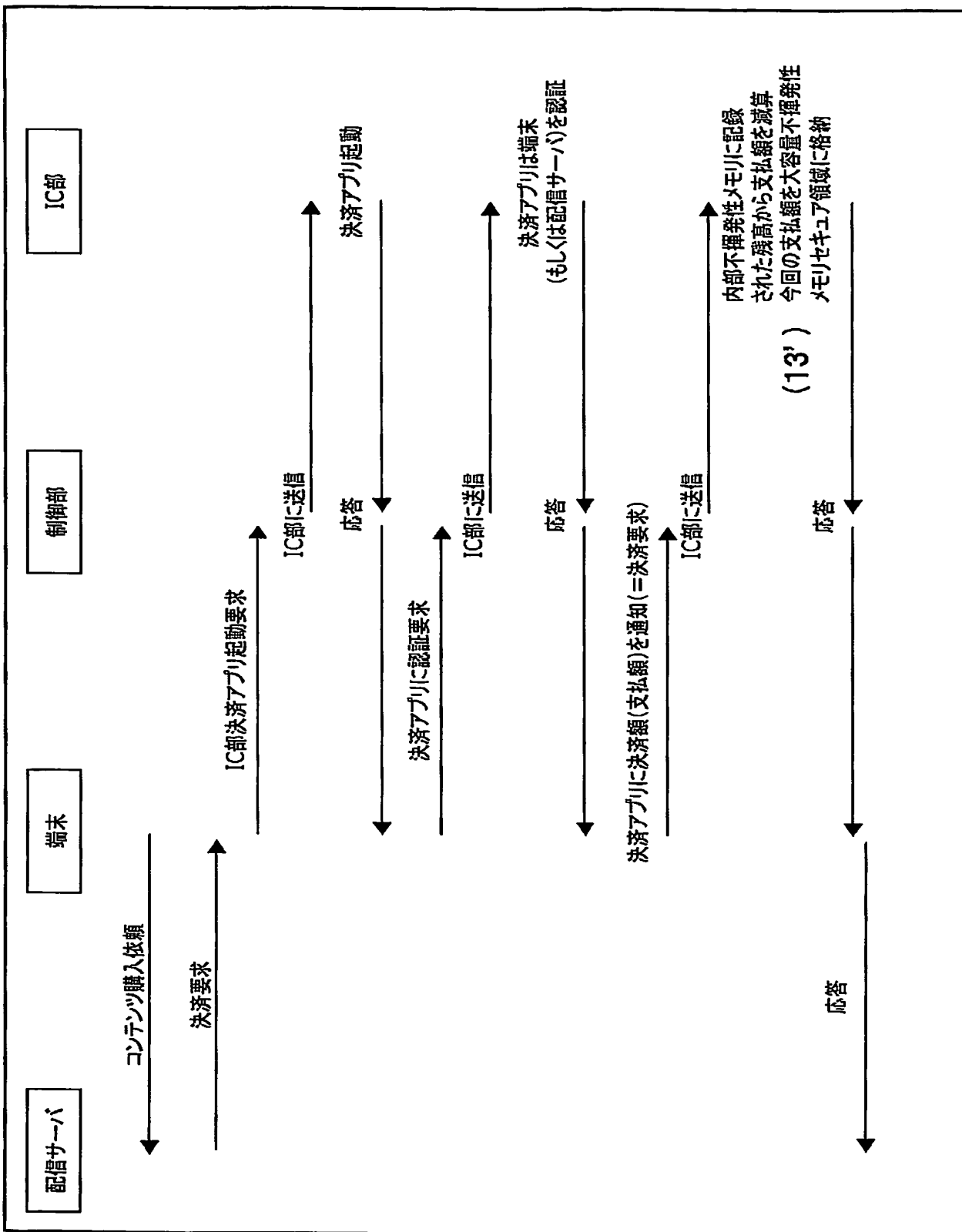


図 8

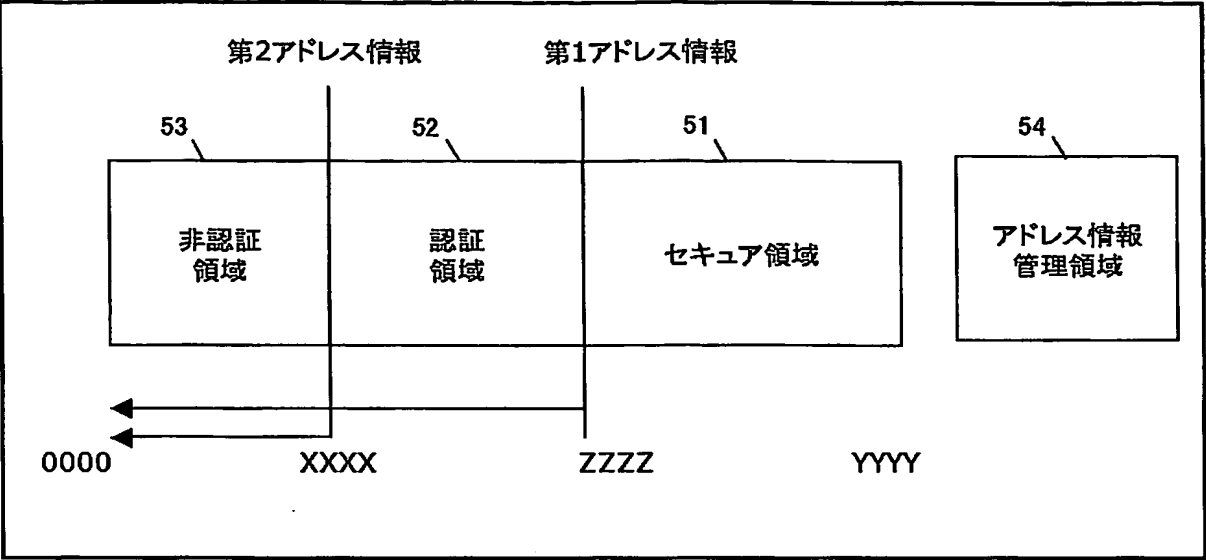


图 9

非認証領域		認証領域		セキユア領域	
論理ブロックNo.	物理ブロックNo.	論理ブロックNo.	物理ブロックNo.	論理ブロックNo.	物理ブロックNo.
0000	0000	0000	EFFF	0000	FFFF
0001	0001	0001	EFFE	0001	FFFE
0002
0003	0003
.	.	.	.	0FFE	F001
.	.	.	.	0FFF	F000
.	.	1FFE	D001		
.	.	1FFF	D000		
CFFE	CFFE				
CFFF	CFFF				

=XXXX-1
相当

=ZZZZ-1
相当

=YYYY
相当

=ZZZZ
相当

=XXXX-1
相当

図 10

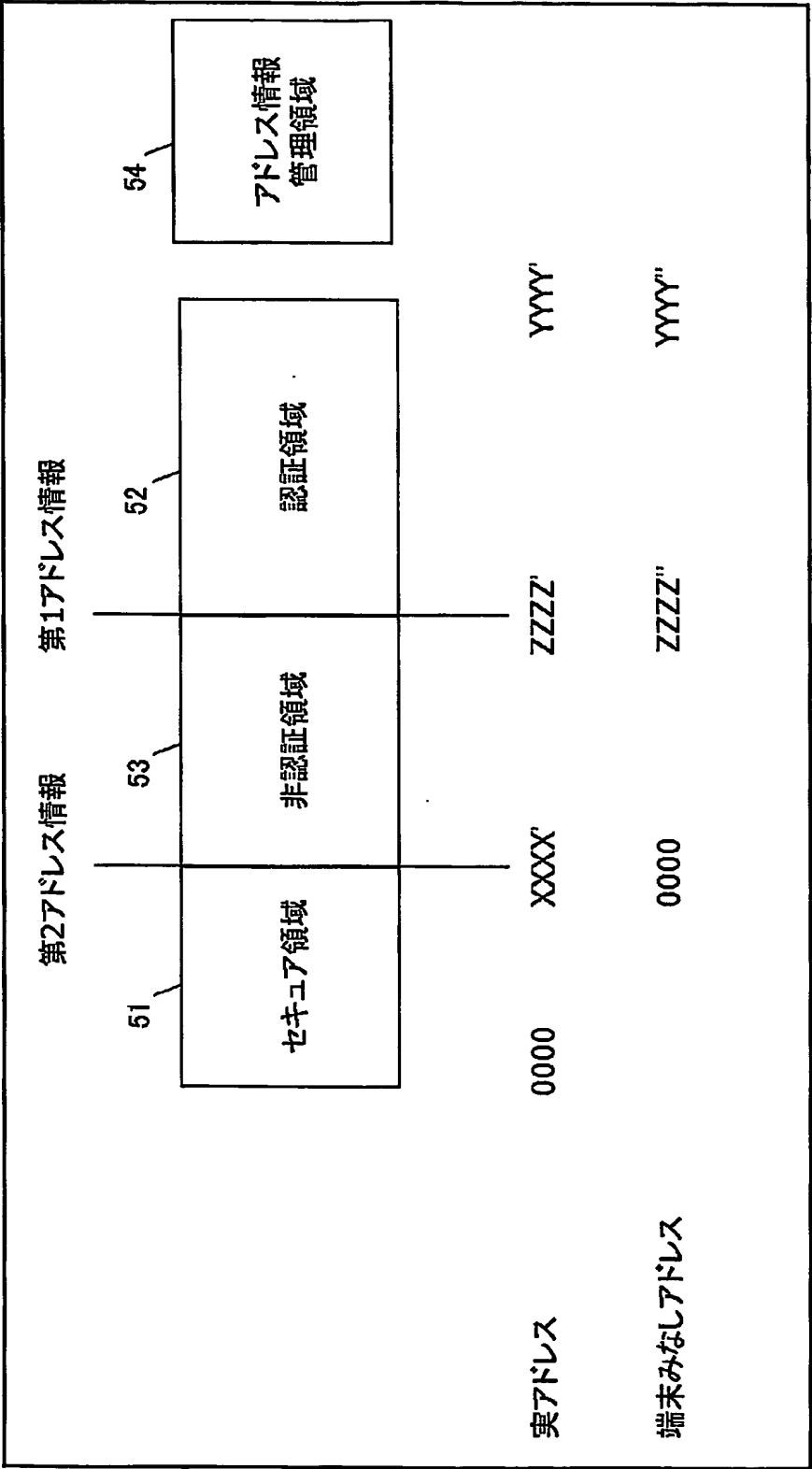


図 1 1

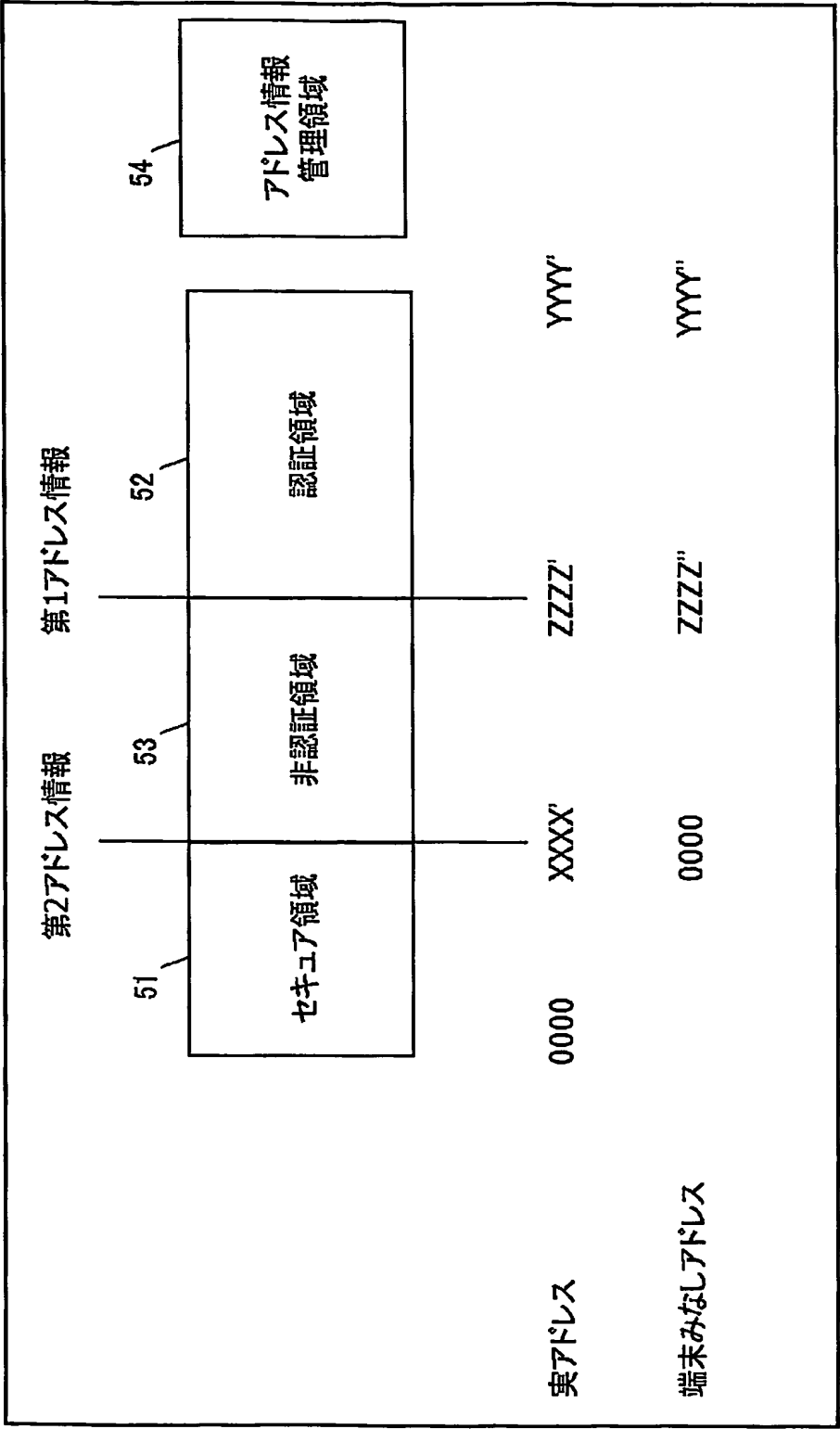


图 12

セキュア領域		非認証領域		認証領域	
論理ブロックNo.	物理ブロックNo.	論理ブロックNo.	物理ブロックNo.	論理ブロックNo.	物理ブロックNo.
0000	0000	0000	D000	0000	FFFF
0001	0001	0001	D001	0001	FFFE
0002	0002
0003	0003
.	.	.	.	0FFE	F001
.	.	.	.	0FFF	F000
.	.	1FFE	EF FE		
.	.	1FFF	EF FF		
CFFE	CFFE				
CFFF	CFFF				

=YYYY'
相当

=ZZZZ'
相当

=ZZZZ'-1
相当

=XXXX'
相当

=XXXX'-1
相当

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/16000

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F12/14, G06K19/073

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F12/14, G06K19/073

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2002-229861 A (Hitachi, Ltd.), 16 August, 2002 (16.08.02), Full text; all drawings & US 2002/169960 A1 & KR 2002065855 A	1-4, 12-15 5-11
Y	JP 2001-14441 A (Matsushita Electric Industrial Co., Ltd.), 19 January, 2001 (19.01.01), Full text; all drawings & EP 1050887 A1 & EP 1050887 B1 & JP 3389186 B2 & JP 2003-233795 A & WO 2000/65602 A1 & AU 200036750 A & CN 1316087 A & KR 2001083073 A & BR 200007581 A	5-11

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
 "E" earlier document but published on or after the international filing date
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 "O" document referring to an oral disclosure, use, exhibition or other means
 "P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
 "&" document member of the same patent family

Date of the actual completion of the international search
10 March, 2004 (10.03.04)

Date of mailing of the international search report
23 March, 2004 (23.03.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))
Int.Cl.⁷ G06F 12/14, G06K 19/073

B. 調査を行った分野
調査を行った最小限資料 (国際特許分類 (IPC))
Int.Cl.⁷ G06F 12/14, G06K 19/073

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
日本国公開実用新案公報 1971-2004年
日本国登録実用新案公報 1994-2004年
日本国実用新案登録公報 1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X Y	JP 2002-229861 A (株式会社日立製作所) 2002.08.16, 全文, 全図 & US 2002/169960 A1 & KR 2002065855 A	1-4, 12-15 5-11
Y	JP 2001-14441 A (松下電器産業株式会社) 2001.01.19, 全文, 全図 & EP 1050887 A1 & EP 1050887 B1 & JP 3389186 B2 & JP 2003-233795 A & WO 2000/65602 A1 & AU 200036750 A & CN 1316087 A & KR 2001083073 A & BR 200007581 A	5-11

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日
10.03.2004

国際調査報告の発送日
23.3.2004

国際調査機関の名称及びあて先
日本国特許庁 (ISA/JJP)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)
桜井 茂行

5N 2945

電話番号 03-3581-1101 内線 3545